UNC SCHOOL OF LAW

NORTH CAROLINA BANKING INSTITUTE

Volume 6 | Issue 1 Article 23

2002

Online Transactions: Squaring the Gramm-Leach-Bliley Act Privacy Provisions with the FTC Fair Information Practice Principles

David Annecharico

Online Transactions: Squaring the Gramm-Leach-Bliley Act Privacy Provisions With the FTC Fair Information Practice Principles

I. INTRODUCTION

In a speech made on the day the Gramm-Leach-Bliley Act (GLBA)[1] was signed, Senator Phil Gramm stated, "[t]here is a nature to things and to society, and as they change, Government has to change to recognize the new reality."[2] The reality of online banking is that the number of people who conduct online transactions is growing exponentially. In August of 2001, there were approximately 13.6 million active Web Bank users in the United States, up from 6.1 million at year-end 1999.[3] These numbers are expected to grow by 16.3 million in the near future.[4] Driven by competition, advances in technology, consumer demand for convenience, and institutional demand for cost-effectiveness, the development of electronic delivery channels for financial services continues to grow at a rapid pace.[5] While these factors

1. Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338-1481 (1999) (codified in scattered sections of 12 U.S.C. & 15 U.S.C.). For an overview of the main provisions of GLBA, see Scott A. Cammarn & Paul J. Polking, *Overview of the Gramm-Leach-Bliley Act*, 4 N.C. BANKING INST. 1 (2000).

2. Press Release, Senate Banking Committee, Gramm Closing Floor Statement on Gramm-Leach-Bliley Act of 1999 (Nov. 4, 1999), *available at* http://banking.senate. gov/prel99/1104sta.htm (last visited Feb. 19, 2002).

3. Press Release, Gomez, Inc., Successful Web Banking Requires Serious Business Discipline (Aug. 20, 2001), *at* http://www.gomez.com/About/releases. asp?art_ID=8211&topcat_id=0&title=yes&subSect=releases (last visited Feb. 19, 2002).

4. *Id.*

5. FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE, A REPORT TO CONGRESS 1 (2000), *available at* http://www.ftc.gov/reports/privacy2000/privacy2000.pdf (last visited Feb. 18, 2002); *see* Press Release, Forrester Research, Inc., Online Retail to Reach $184 Billion by 2004 as Post-Web Retail Era Unfolds (Sept. 1999) (on file with N.C. Banking Institute).

have made e-commerce possible and profitable,[6] they have also enabled financial institutions to collect, analyze, and share vast quantities of personal data taken from consumers who visit their Web sites.[7] The increase in data collection and usage has led to public concerns about misuse of personal information,[8] lack of control over information given during online financial transactions,[9] and the reasons for which personal information is being shared.[10]

This Note addresses the Federal Banking Agencies'[11] (Agencies) guidelines mandated by Title V of GLBA[12] that relate to the regulation and safeguarding of non-public personal information given by consumers who utilize online services.[13] In Part II, this Note provides an overview of the policy debate

6. Press Release, Shop.org News, Online Retailing in North America to Reach $65 Billion In 2001 (May 2, 2001), *available at* http://www.shop.org/press/01/050201.html (last visited Feb. 19, 2002).

7. FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE, A REPORT TO CONGRESS 1 (2000) [hereinafter FAIR INFORMATION PRACTICES], *available at* http://www.ftc.gov/reports/privacy2000/privacy2000.pdf (last visited Feb. 10, 2002).

8. *Id.* at 2 (presenting survey data regarding consumer concerns about misuse of personal information). *See also* John Schwarz, *Government Is Wary of Tackling Online Privacy*, N.Y. TIMES, Sept. 6, 2001, at C1 (characterizing privacy as one of the most challenging issues for policy makers).

9. *See* Forrester Research, Inc., *Forrester Technographics® Finds Online Consumers Fearful Of Privacy Violations* (Oct. 1999) ("Nearly 90% of online consumers want the right to control how their personal information is used after it is collected. . . .") (quoting Christopher M. Kelley, associate analyst in Technographics Data & Analysis), *available at* http://www.forrester.com/ER/Press/Release/0,1769,177,FF.html (last visited Mar. 1, 2002).

10. Sandeep Junnarkar, *Report: Half of Net Users Mistrust Sites,* CNET NEWS.COM (Aug. 17, 1999) (citing results of study by Jupiter Communications, Inc.), *at* http://home.cnet.com//category/0-1007-200-346152.html (last visited Feb. 19, 2002); *see* JUPITER COMMUNICATIONS, INC., OVERVIEW: PROACTIVE ONLINE PRIVACY: SCRIPTING AN INFORMED DIALOGUE TO ALLAY CONSUMER'S FEARS, *available at* http://www.jup.com (last visited Feb. 18, 2002).

11. Gramm-Leach-Bliley Act § 505(a)(1), 15 U.S.C. § 6805(a)(1) (2000). The Federal Banking Agencies are the Office of the Comptroller of the Currency (OCC), the Board of Governers of the Federal Reserve System (FRB), the Board of Directors of the Federal Deposit Insurance Corporation (FDIC), and the Director of the Office of Thrift Supervision (OTC). *Id.*

12. Gramm-Leach-Bliley Act §§ 501-527, 15 U.S.C. §§ 6801-6809, 6821-6827 (2000).

13. *See infra* notes 18-210 and accompanying text.

regarding the privacy provisions of GLBA.[14] In Part III, this note uses Federal Trade Commission (FTC)[15] fair information practice principles to analyze the adequacy of the Agencies' privacy regulations.[16] Finally, in Part IV, the success of the Agencies' regulations in meeting the public demand for privacy is summarized in light of the fair information practice principles, and future legislative developments.[17]

II. OVERVIEW OF THE PRIVACY DEBATE: SETTING THE TONE FOR TITLE V

Before 1995, congressional Internet legislation was mainly concerned with "education," "libraries," and "access to government information."[18] However, in 1996, the 104th Congress initiated a number of attempts to regulate consumer privacy on the Internet.[19] The critical issue regarding privacy regulations, at that time, was the extent and nature of governmental participation in the regulation of the Internet.[20] The 105th Congress resolved this debate by demonstrating a preference for self-regulation initiatives

14. Gramm-Leach-Bliley Act §§ 501-527, 15 U.S.C. §§ 6801-6809, 6821-6827 (2000); *see infra* notes 18-50 and accompanying text.

15. *See* FAIR INFORMATION PRACTICES, *supra* note 7, at i (discussing the fair information practice principles).

16. *See* Gramm-Leach-Bliley Act §§ 505(a)(1), 15 U.S.C. § 6805(a)(1) (2000) (delegating authority to enforce Title V provisions to the Agencies); *see infra* notes 51-210 and accompanying text.

17. *See infra* notes 211-33 and accompanying text.

18. *See* Yochai Benkler, *Symposium Overview: Part IV: How (If At All) to Regulate the Internet: Net Regulation: Taking Stock and Looking Forward*, 71 U. COLO. L. REV. 1203, 1209 (2000) (providing an overview of Internet legislation in the nineties).

19. *See, e.g.*, Social Security Online Privacy Protection Act of 1996, H.R. 4299, 104th Cong. (1996) (regulating the disclosure of social security numbers obtained by interactive computer service); Consumer Internet Privacy Protection Act of 1996, H.R. 4113, 104th Cong. (1996) (addressing the privacy of transactional information). Neither of these bills passed. Social Security Online Privacy Protection Act of 1996, Bill Summary (summarizing bill status), *available at* http://thomas.loc.gov/cgi-bin/bdquery/z?d104:HR04299:@@@L&summ2=m& (last visited Feb. 19, 2002); Consumer Internet Privacy Protection Act of 1996, Bill Summary (summarizing bill status), *available at* http://thomas.loc.gov/cgi-bin/bdquery/z?d104:HR04113:@@@L&summ2=m& (last visited Feb. 19, 2002).

20. *See* Benkler, *supra* note 18, at 1213-16 (providing an overview of Internet legislation enacted by the 104th Congress).

such as requiring federal agencies to comply with the same consumer privacy practices as private businesses.[21]

The FTC, engaged in the online privacy policy debate since 1995, has taken an interest in crafting policy for regulating the privacy aspects of online financial transactions.[22] In a 1998 report, *Privacy Online: A Report to Congress*,[23] the FTC introduced the four substantive fair information practice principles of notice, choice, access, and security. Instead of recommending legislation, the FTC encouraged the online industry[24] to regulate itself by adopting privacy principles using the fair information practice principles as a policy ideal.[25]

Despite the governmental preference for self-regulating initiatives, the American Bar Association Committee on Banking Law noted that a number of class action lawsuits had been filed regarding the sale of consumer financial information.[26] For example, Mike Hatch, Attorney General for the State of Minnesota, filed a major lawsuit against U.S. Bank on June 9, 1999, in the U.S. District Court for the District of Minnesota.[27] U.S. Bank was accused of selling sensitive customer information to

---

21. *See, e.g.*, Practice What You Preach Privacy Protection Promotion Act, H.R. 4632, 105th Cong. (1998) (requires all Federal agencies using electronic media in carrying out their activities to comply with FTC rules for the protection of persons subject to information gathering through such media). This bill did not pass. *See* Practice What You Preach Privacy Protection Promotion Act, H.R. 4632, Bill Summary (summarizing bill history), *available at* http://thomas.loc.gov/cgi-bin/bdquery/z?d105:HR04632:@@@L&summ2=m& (last visited Feb. 19, 2002).

22. *See* FAIR INFORMATION PRACTICES, *supra* note 7, at i (explaining FTC interest in privacy regulation).

23. FED. TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS (June 1998), *available at* http://www.ftc.gov/reports/privacy3/index.htm (last visited Feb. 19, 2002).

24. *See* Courtney Macavinta, *Net Industry Reacts to FTC Threat,* CNET NEWS.COM (June 3, 1998) (reporting industry reaction to FTC introduction of the fair information practice principles), *at* http://news.com.com/2100-1023-211867.html (last visited Feb. 19, 2002).

25. *See* FAIR INFORMATION PRACTICES, *supra* note 7, at 6 (advocating the fair information practice principles as a baseline policy for Internet privacy regulation).

26. AMERICAN BAR ASSOCIATION COMMITTEE ON BANKING LAW, 2000 MIDWINTER REPORT TO THE BAR COUNCIL OF THE AMERICAN BAR ASSOCIATION (Dec. 17, 1999) (citing a number of class actions suits dealing with sales by financial institutions of information to third parties), *available at* http://www.abanet.org/buslaw/reports/2000win/banking_law_2000.html (last visited Feb. 19, 2002).

27. *See* Complaint, Hatch v. United States Bank Nat'l Ass'n. (D. Minn. 1999) (No. 99-872 adm/ajb), *available at* http://www.ag.state.mn.us/consumer/privacy/PR/pr_usbank_06091999.html (last visited Feb. 19, 2002).

a marketing firm without customer knowledge or consent, and they settled the case for four million dollars.[28] Title V of GLBA was included as a response to growing concern that industry efforts to self-regulate consumer privacy were not working to slow the proliferation of privacy litigation.[29]

Signed into law on November 12, 1999, GLBA[30] eliminates depression-era restrictions imposed by the Banking Act of 1933 (Glass-Steagall Act)[31] and permits the creation of financial holding companies.[32] Title V of GLBA[33] protects the privacy of consumer financial information by requiring disclosure policies[34] and limiting instances where information can be shared by affording consumers a chance to opt out[35] of having certain categories of their non-public personal information from being shared.[36] These privacy provisions are the foundation for the regulatory rulemaking[37] and

28. *See* Final Judgment and Order for Injunctive and Consumer Relief, Hatch v. United States Bank Nat'l Assoc. (D. Minn. 1999) (No. 99-872 adm/ajb), *available at* http://www.ag.state.mn.us/consumer/ privacy/pr/us_bank_judgement.html (last visited Feb. 19, 2002).

29. *See* Michael A. Benoit & Nicole F. Munro, *Recent Federal Privacy Initiatives Affecting the Electronic Delivery of Financial Services*, 56 BUS. LAW. 1143, 1144 (2001) (explaining the political environment in which Title V of the GLBA was created).

30. *See generally* Cammarn & Polking, *supra* note 1 (providing an overview of the main provisions of the GLBA).

31. The Banking Act of 1933, Pub. L. No. 73-66, 48 Stat. 162 (1933) (codified in scattered sections of 12 U.S.C.).

32. Gramm-Leach-Bliley Act § 103, 12 U.S.C. § 1843(k) (2000) (enumerating permissible activities for financial holding companies).

33. *Id.* § 501-527, 15 U.S.C. §§ 6801-6809, 6821-6827 (2000).

34. *See id.* § 502, 15 U.S.C. § 6802 (delineating obligations of financial institutions regarding disclosure of personal information).

35. *See id.* § 502(b), 15 U.S.C. § 6802(b) (creating obligation to give consumers the opportunity to opt out, and providing exceptions to the general opt out rule).

36. *See id.* § 502(a), 15 U.S.C. § 6802(a) (2000) (prohibiting disclosure to nonaffiliated third parties); Cammarn & Polking, *supra* 1, at 27.

37. *See* Gramm-Leach-Bliley Act § 504, 15 U.S.C. § 6804 (designating regulatory authority to the Federal banking agencies).

enforcement[38] regime created by the Agencies[39] in 12 C.F.R. parts 40, 216, 332, and 573.[40]

GLBA privacy provisions apply to any institution that engages in activities that are financial in nature,[41] as described in section 4(k) of the Bank Holding Company Act of 1956.[42] Online loan and account applications are considered financial services because the application involves the evaluation and brokerage of information collected in connection with a financial product or service (a loan or account).[43]

Through governing when and how financial institutions[44] and their affiliates[45] share consumer non-public personal

38. *See id.* § 505, 15 U.S.C. § 6805 (designating authority to enforce regulations of the Federal banking agencies to institutions and persons within their respective jurisdictions).

39. *See* Gramm-Leach-Bliley Act § 505(a)(1), 15 U.S.C. § 6805(a)(1) (2000) (delegating the Agencies' authority to enforce Title V provisions).

40. *See* Privacy of Consumer Financial Information; Final Rule, 65 Fed. Reg. 35,162 (June 1, 2000) (codified at 12 C.F.R. pts. 40, 216, 332, 573). In a joint ruling, the Federal banking agencies adopted a uniform set of privacy provisions for the protection of non-public personal information about consumers. *Id.* To avoid redundancy while citing to these uniform provisions, this Note makes reference to Agencies regulations by citation to the applicable Federal Reserve Board regulation. *See* Privacy of Consumer Financial Information; Final Rule, 65 Fed. Reg. 35,162 (June 1, 2000) (codified at 12 C.F.R. pt. 216); Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness; Final Rule, 66 Fed. Reg. 8634 (Feb. 1, 2001) (codified at 12 C.F.R. pts. 208, 211, 225, 263).

41. Gramm-Leach-Bliley Act § 501(b), 15 U.S.C. § 6801(b) (requiring financial institutions to comply with Title V privacy standards); *see id.* §509(3)(A), 15 U.S.C. § 5809(3)(A) (2000) (defining the term 'financial institution); *see also id.* § 505, 15 U.S.C. § 6805 (2000) (outlining jurisdictional lines of enforcement between various regulatory bodies).

42. *See* The Bank Holding Company Act of 1956 § 4(k), 12 U.S.C. § 1843(k) (2000) (defining activities that are financial in nature).

43. *See id.* § 1843(k)(3)(C). According to the Bank Holding Company Act, there are a number of relevant factors to take into account in the determination of whether an activity is financial. *Id.* § 1843(k)(3)(A)-(D). One such factor is "changes or reasonably expected changes in the technology for delivering financial services." *Id.* § 1843(k)(3)(C).

44. *See* Privacy of Consumer Financial Information, 12 C.F.R. § 216.3(k) (2001) (defining financial institution as "any institution the business of which is engaging in activities that are financial in nature or incidental to such financial activities as described in section 4(k) of the Bank Holding Company Act of 1956").

45. *Compare* 12 C.F.R. § 216.3(a) (defining affiliate), *with* 12 C.F.R. § 216.3(m) (defining non-affiliated third party). Note that one exception to the general distinction is where a financial institution and a company that is not affiliated jointly employ an individual. In this case, the company that the person is employed with may

information,[46] the agency regulations embody the two privacy principles of GLBA: notice[47] and opt out.[48] Specifically, financial institutions that share consumer non-public personal information with nonaffiliated third parties must provide consumers with (1) an initial opt out notice of the institution's privacy policy[49] and (2) a reasonable time for the consumer to opt out of any proposed sharing of information with nonaffiliates.[50]

III. A CRITICAL LOOK AT THE REGULATIONS—THE MEANS/ENDS FIT BETWEEN THE FEDERAL BANKING AGENCIES REGULATIONS AND THE FAIR INFORMATION PRACTICE PRINCIPLES

On June 1, 2000, the Agencies published a joint final rule governing the Privacy of Consumer Financial Information,[51] pursuant to section 504 of GLBA.[52] On February 1, 2001, the Agencies published a joint final rule governing standards for the safekeeping of public information,[53] pursuant to sections 501 and 505(b) of GLBA.[54] These joint final rules work in tandem to create a regulatory framework for GLBA's mandate to limit the disclosure of non-public personal information by providing notice,

---

be treated as an affiliate for purposes of sharing nonpersonal information. 12 C.F.R. § 216.3(m)(ii).

46. *See* 12 C.F.R. § 216.3(n) (defining non-public personal information). Note that nonpublic personal information is defined as all personally identifiable information that is not publicly available. 12 C.F.R. § 216.3(n)(1). This subset is extended to include all lists or groupings that were created using non-public information or contain non-public personal information. *Id.* For example, a database listing of consumer names and social security numbers would, itself, be non-public personal information. *Id.*

47. Gramm-Leach-Bliley Act § 502(a), 15 U.S.C. § 6802(a) (2000).

48. *Id.* § 502(b), 15 U.S.C. § 6802(b).

49. Privacy of Consumer Financial Information; Final Rule, 12 C.F.R. § 216.4(a) (2000).

50. 12 C.F.R. § 216.7(a) (2001).

51. Privacy of Consumer Financial Information, 65 Fed. Reg. 35,162 (June 1, 2000) (to be codified at 12 C.F.R. pts. 40, 216, 332, 573).

52. Gramm-Leach-Bliley Act § 504, 15 U.S.C. § 6804 (2000).

53. Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness, 66 Fed. Reg. 8616 (Feb. 1, 2001) (to be codified at 12 C.F.R. pts. 208, 211, 225, 263).

54. Gramm-Leach-Bliley Act §§ 501, 505(b), 15 U.S.C. §§ 6801, 6805(b) (2000).

allowing consumers to opt out, and insuring informational security.[55]

GLBA is clear regarding the jurisdiction of various regulatory bodies.[56] The Agencies are jointly responsible for all federal banking activities;[57] as such, they have the power to regulate the privacy standards for federal banks.[58] GLBA sets the FTC's jurisdiction as all financial institutions that are not covered[59] by other regulatory bodies mentioned in section 505(a).[60]

The FTC has introduced regulations that are identical to the Agencies.[61] In the same month that the FTC issued these regulations, they also released a report reiterating their commitment to the fair information practice principles as a policy ideal for Internet privacy legislation.[62] In this report, the Commission recommended that legislation be enacted, using the fair information practice principles as guidelines by which to create a "basic level of privacy protection for all visitors to consumer-oriented commercial Web sites . . . ."[63] In this respect, the fair

---

55. *Supra* notes 53-54 and accompanying text.

56. *See* Gramm-Leach-Bliley Act § 505(a), 15 U.S.C. 6805(a) (designating jurisdiction to enforce the privacy provisions to various regulatory bodies).

57. *See* Gramm-Leach-Bliley Act § 505(a)(1)(A)-(D) (designating the jurisdiction of the Agencies).

58. *Id.*

59. According to the FTC,

> [t]hese entities include, but are not limited to, mortgage lenders, "pay day" lenders, finance companies, mortgage brokers, non-bank lenders, account servicers, check cashers, wire transferors, travel agencies operated in connection with financial services, collection agencies, credit counselors, and other financial advisors, tax preparation firms, non-federally insured credit unions, and investment advisors that are not required to register with the Securities and Exchange Commission.

THE FTC, FREQUENTLY ASKED QUESTIONS FOR THE PRIVACY REGULATION, *available at* http://www.ftc.gov/privacy/glbact/glb-faq.htm (last visited Feb. 19, 2002).

60. *See* Gramm-Leach-Bliley Act § 505(a)(7), 15 U.S.C. § 6805 (2000) (designating FTC jurisdiction as any other financial institution not covered in subsection 505(a)).

61. *Compare* Privacy of Consumer Financial Information, 65 Fed. Reg. 33,646 (May 24, 2000) (to be codified at 16 C.F.R. pt. 313), *with* Privacy of Consumer Financial Information, 65 Fed. Reg. 35,206 (June 1, 2000) (to be codified at 12 C.F.R. pt. 216).

62. *See* FAIR INFORMATION PRACTICES, *supra* note 7, at 36.

63. *Id.* at 36.

information practice principles were not introduced as regulatory law; rather, they were introduced as a policy ideal through which to structure the confusing legislative landscape dealing with online privacy.[64]

Through the fair information practice principles, the FTC is attempting to lay the policy groundwork for a uniform privacy standard. The FTC's recommendation was made on the basis of a survey of privacy protections used by a random sample of all Web sites with at least 39,000 monthly visitors, as well as the 100 most popular commercial Web sites in the United States.[65] Using a weighted analysis[66] of the pool of Web sites surveyed, the FTC concluded[67] that thirty-two percent had implemented or partially implemented the fair information practice principles.[68] This percentage was seen as an improvement from past years, but still indicated that a small number of Web sites were providing adequate privacy protections in the core areas of notice, choice, access, and security.[69]

Since the publication of the Agencies' regulations, there has been much debate regarding whether GLBA privacy provisions meet increasing public concern regarding the treatment of personal information on the Internet.[70] Throughout these privacy debates, the fair information practice principles have been widely accepted as a gauge by which to measure privacy legislation.[71] In a recent hearing before the Senate Commerce, Science, and Transportation Committee, the common denominator in the public debate over Internet privacy was

64. *See id.* at 37 ("Such rules or regulations could provide further guidance to Web sites by defining fair information practices with greater specificity.").

65. *Id.* at 7.

66. *See id.* at App. A (outlining methodology used for survey).

67. *See id.* at App. B (presenting survey results).

68. *See* FAIR INFORMATION PRACTICES, *supra* note 7, at 12 (summarizing survey results).

69. *Id.* at 12.

70. *See Id.* at 2; *Need for Internet Privacy Legislation: Hearing Before the S. Commerce, Sci. and Transp. Comm.*, 107th Cong. 1 (2001) (statement of Sen. John McCain) (arguing that surveys show that Americans are concerned with online privacy), *available at* http://www.senate.gov/~commerce/hearings/071101jsm.PDF (last visited Feb. 19, 2002) [hereinafter McCain Statement].

71. *See* McCain Statement, *supra* note 70, at 1 (praising the fair information practice principles), *available at* http://www.senate.gov/~commerce/hearings/071101jsm.PDF (last visited Feb. 19, 2002).

recognized as the extent to which existing and proposed legislation meets the notice, choice, access and security standards of the fair information practice principles.[72] The 107th Congress[73] has reacted to public apprehension by introducing a number of bills that seek to modify GLBA to provide heightened notice,[74] greater consumer choice regarding information,[75] consumer access to information,[76] and stricter standards regarding what information may be shared.[77] An examination of existing regulations and the continuing debate regarding the privacy provisions serve to

---

72. *Id.*

73. *See id.* (commenting that recent bills have addressed the fair information practice principles).

74. *See* Privacy Act of 2001, S. 1055, 107th Cong. § 101 (2001) (requiring commercial entities to categorically list the type and uses of information being collected from consumers prior to all sales); Consumer's Right to Financial Privacy Act, H.R. 2720, 107th Cong. § 2 (2001) (amending section 503 of GLBA to require that specific categories of information be included in privacy notices given to consumers).

75. *See* Financial Institutions Privacy Protection Act of 2001, S. 450, 107th Cong. § 3 (2001) (amending section 502 of the GLBA to require consumer opt in consent for information transfers); Consumer's Right to Financial Privacy Act, H.R. 2720, 107th Cong. § 2 (2001) (amending section 502 of GLBA to require consumer opt in consent for information transfers).

76. *See* Financial Information Privacy Act of 2001, S. 30, 107th Cong § 3 (2001) (amending GLBA to allow consumer access to non-public information); Consumer's Right to Financial Privacy Act, H.R. 2720, 107th Cong. § 2 (2001) (amending section 502 of GLBA to allow consumer access to all non-public information received by financial institutions).

77. *See* Social Security Number Privacy Act of 2001, S. 324, 107th Cong. (2001) (amending GLBA to prohibit the sale and purchase of the social security number of individuals by financial institutions); Freedom From Behavior Profiling Act of 2000, S. 536, 107th Cong. (2001) (amending GLBA to limit the sharing of marketing and behavioral profiling information); Financial Information Privacy Act of 2001, S. 30, 107th Cong. § 3 (2001) (amending section 502(b) of GLBA to restrict the transfer of information about personal spending habits); Financial Information Privacy Act of 2001, S. 30, 107th Cong § 4 (2001) (amending section 502(c) of GLBA to restrict the use of health information in making credit and other financial decisions).

illustrate that the FTC's[78] fair information practice principles[79] may be emerging as a policy ideal[80] that will frame future legislation.

A. Notice

According to the FTC fair information practice principle of notice, Web sites should be required to provide consumers with a clear and conspicuous notice of all information practices.[81] This includes identification of what institutions are collecting data, the uses to which the data will be put, recipients of the data, the nature of the data collected and the means by which it is collected.[82] Furthermore, notice requires that an institution reveal whether provision of personal data is voluntary or required and the steps to insure data security.[83]

According to the Agencies' regulations, the initial obligation to a Web site visitor depends upon whether the individual is a consumer or a customer.[84] This classification is based upon the type of relationship that exists between a bank and the individual.[85] Generally, a consumer is defined as "any individual who applies for or obtains a financial product or service from a financial institution for personal, family or household purposes."[86] In this context, any individual who provides non-

78. Two of the bills introduced in the 107th Congress give the FTC heightened enforcement authority. *See* Financial Information Privacy Act of 2001, S. 30, 107th Cong. § 7 (2001) (amending section 505 of GLBA to heightened enforcement rights by the FTC); Privacy Act of 2001, S. 1055, 107th Cong. § 102(a) (2001) (granting the FTC authority to enforce any violations under the act).

79. *See* FAIR INFORMATION PRACTICES, *supra* note 7, at 4 (discussing the fair information practice principles).

80. *See Need for Internet Privacy Legislation: Hearing Before the S. Commerce, Sci. and Transp. Comm.*, 107th Cong. 2 (2001) (statement of Sen. John McCain, commenting that recent bills have addressed the fair information practice principles), *available at* http://www.senate.gov/~commerce/hearings/071101jsm.PDF (last visited Feb. 19, 2002).

81. *See* FAIR INFORMATION PRACTICES, *supra* note 7, at 14 (defining the Fair Information Principle of notice).

82. *Id.*

83. *Id.*

84. *Compare* Privacy of Consumer Financial Information, 12 C.F.R. § 216.3(e) (2001) (providing a definition of consumer), *with* Privacy of Consumer Financial Information, 12 C.F.R. § 216.3(h) (2001) (providing a definition of customer).

85. 12 C.F.R. § 216.3(e), (f).

86. *Id.* § 216.3 (e)(1).

public personal information for an online financial service that involves an examination of credit,[87] a determination of loan qualification,[88] or a request for financial advice[89] is deemed to be a consumer. Customers are defined as the subset of consumers who develop a continuing relationship with a bank.[90] In this context, the individual who then opens a deposit or investment account,[91] obtains a loan,[92] or receives financial advice for a fee[93] is deemed to be a customer.

The general rule is that a single loan creates one customer relationship, which is attached to the institution that services the loan.[94] This rule makes it possible for a single loan to create one customer relationship, but many consumer relationships. For example, if a bank sells a loan to another bank, but keeps the servicing rights, a customer relationship is created with the original bank and a consumer relationship is created with the bank that bought the loan.[95]

The status distinction between customer and consumer determines the level of notice that an individual is entitled to receive. A customer is entitled to receive a full privacy notice;[96] the Agencies' full privacy notice conforms well to the fair information practice principle of notice. The content of a full privacy notice can be divided into nine general categories of informational disclosure.[97] The first three categories concern privacy related information itself. Specifically, a financial institution must disclose all non-public personal information that it: (1) collects;[98] (2) plans to disclose;[99] and (3) collects and discloses about former customers.[100] The next three categories

87. *See, e.g., id.* § 216.3 (e)(2)(i).
88. *See, e.g., id.* § 216.3 (e)(2)(ii).
89. *See, e.g., id.* § 216.3 (e)(2)(iii).
90. Privacy of Consumer Financial Information, 12 C.F.R. § 216.3(e), (h) (2001).
91. *See, e.g., id.* § 216.1(i)(2)(i)(A) (2001).
92. *See, e.g., id.* § 216.1(i)(2)(i)(B).
93. *See, e.g., id.* § 216.1(i)(2)(i)(H).
94. *Id.* § 216.3(e)(2)(iv) (2001).
95. *See, e.g., id.* § 216.3(h)(ii)(B).
96. Privacy of Consumer Financial Information, 12 C.F.R. § 216.4(a)(1) (2001).
97. *Id.* § 216.6(a)(1)-(9) (2001).
98. *Id.* § 216.6(a)(1).
99. *Id.* § 216.6(a)(2).
100. *Id.* § 216.6(a)(3).

relate to how and with whom the financial institution shares information. Specifically, a financial institution must disclose: (4) affiliated and third party recipients of information;[101] (5) all joint servicing and marketing agreements;[102] and (6) affiliate sharing under the Fair Credit Reporting Act.[103] The final three categories relate to disclosure of: (7) information security practices;[104] (8) notice of the right to opt out;[105] and (9) the fact that a financial institution may make disclosures about personal information to entities other than provided by the notice, if provided by law.[106] These nine categories insure that a clear and concise statement regarding information practices is communicated to customers.[107]

GLBA's notice obligation to consumers does not meet the fair information practice principles standard. While a customer is entitled to receive a full privacy notice, consumers are entitled to receive notice only if the institution intends to share non-public personal information.[108] Furthermore, the Agencies regulations abridge the form and content of initial notices to consumers by allowing a "short form" of the full notice to be given in lieu of a full privacy notice.[109] This notice must (1) be clear and conspicuous,[110] (2) include a statement that the consumer can obtain a copy of the full privacy notice,[111] and (3) provide instructions on how to request such a full privacy notice.[112] While the Agencies require a clear and conspicuous notice of all information practices,[113] the short form notice does not identify

101. *Id.* § 216.6(a)(4).

102. Privacy of Consumer Financial Information, 12 C.F.R. § 216.6(a)(5) (2001).

103. *Id.* § 216.6(a)(7).

104. *Id.* § 216.6(a)(8).

105. *Id.* § 216.6(a)(6).

106. *Id.* § 216.6(a)(9).

107. *See id.* § 216.4(a) (requiring that banks provide clear and conspicuous notice).

108. Privacy of Consumer Financial Information; Final Rule, 12 C.F.R. § 216.4(b)(1) (2001).

109. *Id.* § 216.6(d) (2001).

110. *Id.* § 216.6(d)(2)(i).

111. *Id.* § 216.6(d)(2)(ii).

112. *Id.* § 216.6(d)(2)(iii); *see id.* § 216.6(d)(3) (requiring that a bank need only provide a reasonable means through which consumers may obtain the full privacy notice).

113. *See* Privacy of Consumer Financial Information; Final Rule, 12 C.F.R. § 216.4(a)(1) (2001) (requiring clear and conspicuous notice to consumers that accurately reflects privacy policies and practices).

what institutions are collecting data, the uses to which the data will be put, recipients of the data, the nature of the data collected and the means by which it is collected.[114] Furthermore, the short form notice does not obligate an institution to reveal whether provision of personal data is voluntary or required, or what steps are being taken to insure data security.[115]

The difference between notice obligations to customers and consumers illustrates that consumers receive very little in the way of initial notice and must take additional steps to obtain important information regarding what non-public personal information could potentially be shared. While the Internet promises to be a swift paperless conduit for information transfers, requiring consumers to take additional steps to obtain full privacy notices may be confusing and inconvenient in the context of online transactions. The regulations allow delivery of initial privacy notices to be made electronically,[116] but only under circumstances where the consumer has obtained a financial product or service electronically.[117] The general rule is that a bank's Web site must post the privacy notice and require that a consumer acknowledge receipt before obtaining a particular financial service.[118] Here, a short form notice may be flashed on a consumer's computer screen, only to disappear with the click of a mouse. Furthermore, the consumer must arrange to visit the Web site where a full privacy notice is located. If there is no Web site where the full privacy notice is located, the consumer may have to call a toll free number to request a full privacy notice. The fair information practice principle of notice would require

114. *Id.* § 216.7(a)(1)(i)-(iii) (2001).

115. *Compare* 12 C.F.R. § 216.7 (designating the form of opt out notice to be given to consumers), *with* 12 C.F.R. § 216.6 (2001) (designating the information to be included in full privacy notices).

116. *Id.* § 216.9(a) (2001).

117. *Id.* § 216.9(b)(2)(ii). Notices sent via email do not satisfy the requirement that financial institutions transmit notices via channels through which they can reasonably expect that a consumer will receive actual notice. However, if the financial service was obtained electronically, then the notice can be sent electronically. *See Id.* (making electronic delivery unreasonable only in cases where the consumer did not obtain a financial service electronically).

118. *Id.* § 216.9(b)(1)(iii); *see also* Privacy of Consumer Financial Information, 65 Fed. Reg. 35,162, 35,178 (June 1, 2000) (explaining Federal Reserve Board policy as concerns the delivery of privacy notices via the World Wide Web).

financial institutions to give full privacy notices to consumers.[119] The Federal Reserve Board has created a mock online financial institution[120] where administrators may view an example of a full privacy statement that conforms to the regulations.[121]

B. Choice

The fair information practice principle of choice requires banks to afford consumers the "opportunity to consent to secondary uses of information."[122] This principle includes consumer choice regarding internal secondary uses[123] (marketing other products back to customers) and external secondary uses[124] (disclosing data to other entities). The issue of choice is one that consumers have demonstrated concern over.[125]

The Agencies' regulations provide an opt out[126] model through which consumers may choose[127] to inform a bank not to disseminate non-public personal information. Under the opt out model, a bank must provide a reasonable opportunity[128] for a consumer to direct the bank not to disclose non-public personal

---

119. *Compare* FAIR INFORMATION PRACTICES, *supra* note 7, at 14 (defining the Fair Information Principle of notice), *with supra* notes 94-107 and accompanying text (illustrating the Agencies' standards for full privacy notices).

120. FEDERAL RESERVE, THE CHECKER'S BANK, at http://www.federalreserve.gov/tcb/home.html (last visited Feb. 28, 2002). "The Checkers Bank is a simulated web site created by the Federal Reserve to illustrate consumer regulation issues." *Id.*

121. FEDERAL RESERVE, THE CHECKER'S BANK: PRIVACY STATEMENT (providing a full privacy notice), http://www.federalreserve.gov/tcb/aboutus/privacy/privacy.html (last visited Feb. 19, 2002).

122. FAIR INFORMATION PRACTICES, *supra* note 7, at 15.

123. *Id.* at 15.

124. *Id.* at 15-16.

125. *See* Forrester Research, Inc., *supra*, note 9 (concluding that approximately 90% of consumers want to choose how their personal information is used after it is collected), *available at* http://www.forrester.com/ER/Press/Release/0,1769,177,FF.html (last visited Feb. 19, 2002).

126. *See* Privacy of Consumer Financial Information, 12. C.F.R. § 216.10 (2001) (creating limits on disclosure of non-public personal information via an opt out model).

127. *See id.* § 216.10(a)(1) (making consumer failure to opt out as a necessary condition for disclosure).

128. *Id.* § 216.10(a)(1)(iii).

information to nonaffiliated third parties.[129] A bank provides a consumer with this reasonable opportunity if it requires the consumer to decide, as a necessary part of a transaction, whether to opt out before completion of the transaction.[130]

However, in sections 216.13,[131] 216.14,[132] and 216.15,[133] the regulations codify a number of exceptions that GLBA makes to the general prohibition against dissemination of non-public information to nonaffiliated third parties.[134] Categories of non-public information that fall within this exception are permissibly shared with nonaffiliated parties whether or not a consumer chooses to opt out. These exceptions abridge a consumer's choice over information sharing in a number of ways.[135]

For example, section 216.13 allows information sharing between financial institutions that have entered into joint servicing or marketing agreements.[136] A joint agreement is defined as a written contractual[137] relationship between the financial institution and another party whereby the parties "jointly offer, endorse, or sponsor a financial product or service."[138] Information sharing within these types of relationships is acceptable, so long as the relationship is disclosed in the financial institution's full privacy

129. *See id.* § 216.10(a)(2) ("Opt out means a direction by the consumer that you not disclose non-public personal information about that consumer to a nonaffiliated third party, other than as permitted by §§ 216.13, 216.14, and 216.15.").

130. *See id.* § 216.10(a)(3)(iii) (defining reasonable opportunity in the context of isolated consumer transactions).

131. *See* Privacy of Consumer Financial Information; Final Rule, 12 C.F.R. § 216.13 (2001) (detailing exceptions to opt out requirements for service providers and joint marketing).

132. *See id.* § 216.14 (detailing exceptions to notice and opt out requirements for processing and servicing transactions).

133. *See id.* § 216.15 (detailing other exceptions to notice and opt out requirements).

134. *See* Gramm-Leach-Bliley Act § 501(a), 15 U.S.C. 6801(a) (2000) (stating the general privacy policy to be an affirmative obligation to respect the privacy of non-public personal information).

135. *See supra* notes 131-34 and accompanying text (illustrating various exceptions to opt out requirements).

136. *See* Privacy of Consumer Financial Information, 12 C.F.R. § 216.13 (2001) (detailing the exception to opt out requirements for service providers and joint marketing).

137. *See id.* § 216.13(a)(ii) (requiring the joint agreement to be contractual).

138. *Id.* § 216.13(c) (defining the term "joint agreement").

notice[139] and the parties enter into a contractual confidentiality agreement.[140]

Also, section 216.14 reduces consumer choice regarding information sharing for the purpose of processing and serving of transactions.[141] Specifically, an initial privacy notice is not required when information sharing is necessary to "effect, administer or enforce a transaction that a consumer requests or authorizes, or in connection with . . ."[142] (1) servicing or processing a product or service,[143] (2) maintaining or serving the consumers account,[144] or (3) conducting a secondary market sale.[145]

Finally, section 216.15 details exceptions that apply to specific organizations and situations.[146] Financial institutions may share non-public personal information at the consent or direction of the consumer,[147] to protect the security of records,[148] prevent fraud[149] or resolve consumer disputes.[150] Financial institutions may also share information for the function of institutional risk control[151] and to individuals who have a legal, beneficial, fiduciary or representative interest in the customer.[152] Institutions may share non-public personal information with federal, state and local agencies in order to protect public safety.[153] Disclosure in this respect must be in accordance with the Right to Financial Privacy

---

139. *See id.* § 216.13(a)(i) (requiring the bank to provide an initial privacy notice in conformity with section 216.4).

140. *See id.* § 216.13(a)(ii) (requiring the joint agreement to limit informational use to the purpose for which it was given).

141. *See* Privacy of Consumer Financial Information, 12 C.F.R. § 216.14 (2001) (noting exceptions to notice and opt out requirements in cases of processing and servicing transactions).

142. *Id.* § 216.14(a).

143. *Id.* § 216.14(a)(1).

144. *Id.* § 216.14(a)(2).

145. *Id.* § 216.14(a)(3).

146. *See* Privacy of Consumer Financial Information, 12 C.F.R. § 216.15 (2001) (listing other exceptions to notice and opt out requirements).

147. *Id.* § 216.15(a)(1) (2001).

148. *Id.* § 216.15(a)(2)(i).

149. *Id.* § 216.15(a)(2)(ii).

150. *Id.* § 216.15(a)(2)(iii).

151. *See id.* § 216.15(a)(3) (allowing exception to provide information to insurance advisory organizations and organizations that enforce institutional compliance).

152. *Id.* § 216.15(a)(2)(iv).

153. *See* Privacy of Consumer Financial Information, 12 C.F.R. § 216.15(a)(4) (2001) (allowing exception to provide information to state authorities).

Act of 1978.[154] Finally, institutions may share information with consumer reporting agencies[155] in accordance with the Fair Credit Reporting Act.[156]

The Agencies' regulations also limit how banks and nonaffiliated third parties can reuse and redisclose non-public personal information.[157] Specifically, the regulations limit the ways that financial institutions that receive non-public personal information under the exceptions outlined in sections 216.14 and 216.15 may reuse or redisclose that information.[158] A financial institution that receives non-public personal information may only redisclose to it's own affiliates,[159] or to the affiliates of the financial institution from whom the information was initially disclosed.[160] If the financial institution chooses to share information with its own affiliates, then those affiliates can disclose to the same extent that the financial institution may disclose the information.[161] A financial institution can also disclose information received if it is in the ordinary course of business to carry out an activity covered by sections 216.14 or 216.15 under which the information was originally received.[162] Like the abridgments to consumer choice outlined in 216.13,[163] 216.14[164] and 216.15,[165] a consumer has no

154. Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401-3422 (2000). The Right to Financial Privacy Act of 1978 defines government authority to be "any agency or department of the United States, or any officer, employee, or agent. . . ." *Id.* § 3401(3).

155. 12 C.F.R. § 216.15(a)(5).

156. 15 U.S.C. § 1681(b) (2000) (defining the purpose of the Fair Credit Reporting Act to "adopt reasonable procedures for meeting the needs of commerce for consumer credit. . . .").

157. *See* Privacy of Consumer Financial Information; Final Rule, 12 C.F.R. § 216.11 (2001) (delineating the limits on redisclosure and reuse of information).

158. *See id.* § 216.11(a)(1) (delineating standards of redisclosure and reuse of information obtained through sections 216.14 and 216.15).

159. *Id.* § 216.11(a)(1)(ii).

160. *Id.* § 216.11(a)(1)(i).

161. *See id.* § 216.11(a)(1)(ii) (restricting affiliate information reuse to the extent that the original bank could disclose and use the information).

162. *Id.* § 216.11 (a)(1)(iii).

163. *See* Privacy of Consumer Financial Information, 12 C.F.R. § 216.13 (2001) (detailing exceptions to opt out requirements for service providers and joint marketing).

164. *See id.* § 216.14 (providing exception to notice and opt out requirements for processing and servicing transactions).

165. *See id.* § 216.15 (noting other exceptions to notice and opt out requirements).

choice over the extent to which non-affiliates who obtain information may reuse or redisclose that information.

Perhaps the most notable exception to the regulation's standards of choice may be found in the provision of GLBA that relates to a state's right to create additional prohibitions to the protection and dissemination of non-public information.[166] This provision creates a ground floor level of protection, while allowing state legislatures to add additional strictures without fear of federal preemption.[167] In the future, state legislatures may consider this exception to ratchet up consumer choice via an opt in model.[168] In California, a proposal to create an opt in standard was recently defeated.[169] This bill would have required opt out for the generally unrestricted sharing among affiliates afforded by GLBA[170] and opt in for sharing with non-affiliated third parties (GLBA requires opt out in this type of circumstance).[171] It is likely that similar bills will be introduced in the California Legislature, as well as in the U.S. Congress in 2002.[172] The opt out versus opt in model is one of the most frequently debated issues regarding consumer choice.

---

166. *See* Gramm-Leach-Bliley Act § 507, 15 U.S.C. § 6807 (2000) (allowing greater protection under state law); 12 C.F.R. § 216.17 (providing greater protection under state law).

167. Privacy of Consumer Financial Information, 12 C.F.R. § 216.17(b) (2001).

168. *See* STAR SYSTEMS, FINANCIAL PRIVACY: BEYOND TITLE V OF GRAMM-LEACH-BLILEY 24 (providing an overview of state reaction to the GLBA opt out provisions), *available at* http://www.star-systems.com/news-industryresearch.html (last visited Feb. 19, 2002).

169. Financial Information Privacy Act of 2002, S.B. 733, 151st Leg., Reg. Sess. (CA. 2001), *at* http://www.leginfo.ca.gov/pub/bill/sen/sb_0751-0800/sb_773_bill_20010913_amended_asm.pdf (last visited Feb. 19, 2002); *see also* Legislative History of Financial Information Privacy Act of 2002 (detailing the full legislative history of the Financial Information Privacy Act of 2002), *available at* http://www.leginfo.ca.gov/pub/bill/sen/sb_0751-0800/sb_773_bill_20020110_history.html (last updated September 14, 2001).

170. Gramm-Leach-Bliley Act § 502(b)(1), 15 U.S.C. § 6802(b)(1) (2000) (making the general opt out requirement to include information shared with nonaffiliated third parties only).

171. *See id.* § 502(b)(1)(A)-(C), 15 U.S.C. § 6802(b)(1)(A)-(C) (requiring financial institutions to give consumers the opportunity to opt out of information shared with nonaffiliated third parties).

172. *See, e.g.*, Financial Institutions Privacy Protection Act of 2001, S. 450, 107th Cong. § 3 (2001) (amending section 502 of GLBA to require consumer opt in consent for information transfers); Consumer's Right to Financial Privacy Act, H.R. 2720, 107th Cong. § 2 (2001) (amending section 502 of GLBA to require consumer opt in consent for information transfers).

Under the opt in standard, if a consumer does not respond to a notice then the institution cannot use non-public personal information. Under the opt in system, customers who do not respond are assumed to have withdrawn consent.[173] Critics of the opt in model have pointed to potential inefficiency in getting consumers to focus on the opt in choice.[174] There is also reason to believe that opt in models will be more costly for institutions to enact.[175] Another criticism leveled against the opt in approach is that it may pose a significant First Amendment[176] issue by burdening the communication of basic information.[177] However, there is some indication that the courts would consider the nature of the communications.[178] A recent district court case, involving the FTC, indicates that district courts may be willing to uphold privacy regulation where the speech involved is purely commercial.[179] While GLBA's opt out model seems to give consumers reasonable control over the extent to which non-public information is shared, the debate continues over whether an opt in model would actually allow greater consumer control.[180]

The fair information practice principle of choice requires that consumers be given control over how non-public personal

---

173. *Id.*

174. *See* STAR SYSTEMS, *supra* note 168, at 27 (critiquing the opt in model).

175. *See id.* (arguing that under an opt in model, the average household would lose two hundred dollars a year).

176. U.S. CONST. amend. I.

177. *Need for Internet Privacy Legislation: Hearing Before the S. Commerce, Sci. and Transp. Comm.*, 107th Cong. 1 (2001) (statement of Fred Cate) (arguing that opt in models pose First Amendment Issues), *available at* http://www.senate.gov/~commerce/hearings/071101Cate.PDF (last visited Feb. 19, 2002).

178. Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc., 472 U.S. 749, 759 & n.5 (1985) (identifying commercial speech as occupying a subordinate position in First Amendment values); Central Hudson Gas & Electric Corp. v. Public Serv. Comm'n, 447 U.S. 557 (1980) ("[T]he Constitution accords a lesser protection to commercial speech than to other constitutionally guaranteed expression . . . .").

179. *See* Individual Ref. Serv. Group, Inc. v. FTC, 145 F. Supp 2d 6, 40 (D.D.C. 2001) (holding that the FTC's privacy regulations did not violate a credit reporting agency's right to free speech under the First Amendment).

180. *See* STAR SYSTEMS, *supra* note 168, at 27 (providing an overview of the opt out versus opt in debate); *Need for Internet Privacy Legislation: Hearing Before the S. Commerce, Sci. and Transp. Comm.*, 107th Cong. 1 (2001) (statement of Fred Cate) (critiquing the opt in model), *available at* http://www.senate.gov/~commerce/hearings/071101Cate.PDF (last visited Feb. 19, 2002).

information is used by financial institutions.[181] Under GLBA, a consumer does not have the choice to opt out of joint marketing agreements.[182] In this scenario, it is possible that the personal information proffered by a consumer for a loan approval may be used to solicit the consumer for insurance or a credit card. While GLBA requires that disclosure of joint marketing agreements be made in the full privacy notice[183] and that joint marketers may enter into a confidentiality agreement,[184] a consumer's power of choice is nonetheless reduced.[185] Furthermore, without taking extra steps to receive the full privacy notice, a consumer will not be able to deduce that the financial provider is sharing information with a joint marketer via the short form notice.[186]

C. *Access*

The fair information practice principle of access would require Web sites to offer consumers reasonable access to information collected about them.[187] This includes providing a reasonable opportunity to correct errors or delete information.[188]

The Agencies' regulations do not conform to the fair information practice principle of access because there is no provision in GLBA that requires consumers be given access to information gathered about them.[189] Under the regulatory regime created by Title V, once a consumer declines to opt out, the

181. *See* FAIR INFORMATION PRACTICES, *supra* note 7, at 15 (defining the fair information practice principle of choice).

182. *See* Privacy of Consumer Financial Information, 12 C.F.R. § 216.13 (2001) (delineating exceptions to opt out requirements for service providers and joint marketing).

183. *See supra* notes 96-109 (providing an overview of the full privacy notice requirements).

184. *See supra* note 182 and accompanying text.

185. *See supra* notes 131-33 and accompanying text.

186. The regulations do not require financial institutions to specifically name the third parties with whom that institution is sharing information. *See supra* notes 109-13 and accompanying text (providing an overview of the short form privacy notice requirements).

187. *See* FAIR INFORMATION PRACTICES, *supra* note 7, at 16 (defining the fair information practice principle of access).

188. *Id.* at 16.

189. *See generally* Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338-1481 (1999) (codified in scattered sections of 12 U.S.C. & 15 U.S.C.).

information need not be accessible.[190] The opt out provisions do allow banks to opt out of disclosure of certain non-public information and disclosure to nonaffiliated third parties;[191] this partial opt out is at the bank's election.[192]

Legislative activity in the 107th Congress illustrates that federal lawmakers have been challenged to provide a reasonable means for consumers to access non-public personal information given to financial institutions. A number of bills introduced by the House and Senate in 2001 seeks to amend GLBA to give consumers access to information provided to financial institutions.[193]

In the context of online transactions, organizing consumer access to information may be as simple as creating Web based user-name and password permissions for consumers to access their personal information online. The technology is available to conveniently automate the task of logging in and viewing or correcting personal account information.[194]

D Security

The fair information practice principle of security would require Web sites to protect personal information against unauthorized access, use, disclosure, loss or destruction.[195] While

190. Privacy of Consumer Financial Information, 12 C.F.R. §§ 216.1-216.18 (2001). The joint final rule, issued by the Agencies, does not contain a provision dealing with a consumer's right to access her information. *See id.*

191. *See id.* § 216.10(c) (allowing banks to choose a partial opt out plan).

192. *See id.* § 216.10(c) (explaining that a bank may elect to allow consumers to choose to opt out of certain categories of information and nonaffiliated third parties).

193. *See* Financial Information Privacy Protection Act of 2001, S. 30, 107th Cong § 3 (2001) (amending GLBA to allow consumer access to non-public information); Consumer's Right to Financial Privacy Act, H.R. 2720, 107th Cong. § 2 (2001) (amending section 502 of GLBA to allow consumer access to all non-public information received by financial institutions).

194. *See* ASPWIRE.COM, ABOUT ASPWIRE ("(ASP) is an open Web application platform that combines server scripting with custom server components to create browser-independent Web solutions and publish legacy databases to the Web."), *at* http://www.aspwire.com/about.asp (last visited Feb. 19, 2002); Press Release, Macromedia.com, Macromedia Announces Free Coldfusion 5 Developer Edition (Jan. 7, 2002) ("ColdFusion Server 5 provides the most approachable, cost-effective solution for creating interactive user experiences."), *at* http://www.macromedia.com/macromedia/proom/pr/2002/free_cf5.html (last visited Feb. 19, 2002).

195. *See* FAIR INFORMATION PRACTICES, *supra* note 7, at 19 (defining Security as a fair information practice principle).

privacy relates to what information may be used and shared, security refers to the ability to protect that information from illegal access. It is in this way that adequate security measures go hand in hand with safeguarding information deemed to be private.

Pursuant to GLBA, banks must create administrative, technical and physical safeguards for customer records and information.[196] On February 1, 2001, the Agencies published their joint final rule on guidelines for establishing standards through which this requirement is met.[197] The responsibility to create and oversee an information security program[198] that is geared to eliminate foreseeable risks[199] falls upon the board of directors of a financial institution.[200] The specific objectives of this security program are to ensure the confidentiality of customer information, protect against anticipated threats and guard against unauthorized access.[201]

However, the status distinction between customers and consumers determines the level of security that private information is afforded. According to the joint final ruling, the most reasonable interpretation of Title V is that a financial institution is obligated to protect the security and confidentiality of consumers with whom a customer relationship has been established.[202] The joint final rule does not require banks to create security and confidentiality standards for non-public consumer information.[203] A bank must, however, disclose whether or not

196. Gramm-Leach-Bliley Act § 501(b), 15 U.S.C. § 6801(b) (2000).

197. Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness, 66 Fed. Reg. 8634 (Feb. 1, 2000) (to be codified at 12 C.F.R. pts. 208, 211, 225, 263).

198. *Id.* § 208 app. D-2(III) (detailing standards for the creation of an informational security program).

199. *Id.* § 208 app. D-2(III)(B)(1) (requiring an assessment of reasonably foreseeable risks as part of information security programs).

200. *Id.* § 208 app. D-2(III)(A) (making the board of directors of each bank responsible for the creation of an information security program).

201. *Id.* § 208 app. D-2(II)(B) (enumerating the primary objectives of an information security program).

202. Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness, 66 Fed. Reg. 8618 (Feb. 1, 2000) (interpreting Title V to create an obligation to customers only).

203. *See id.* (suggesting that, as a practical matter, financial institutions may also design an information security program for consumers).

there is an information security program,[204] as well as who is authorized to have access to the information.[205] Unfortunately, this disclosure is not made in the short form privacy notice that consumers receive.[206] Rather, information relating to a financial institutions security program appears in the full privacy notice that consumers must take extra steps to receive.[207] For these reasons, customers are entitled to greater security protections than consumers.

The Agencies regulations regarding security, therefore, do not conform to the fair information practice principle of security in so far as they guarantee consumers the same level of protection of personal information against unauthorized access, use, disclosure, loss or destruction. In the context of online transactions, financial institutions may consider researching the option of keeping consumer information in the same secure location that customer information is kept.[208] Customer information, garnered online, is kept in databases or servers located in secure locations.[209] It may be a small and efficient step to require financial institutions to maintain consumer information in the same secure location that customer information is kept.[210]

---

204. Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness, 12 C.F.R. § 216.6(c)(6)(ii) (2001).

205. *Id.* § 216.6(c)(6)(i).

206. The short form notice is not required to disclose the existence of an information security program or who has access to non-public personal information. *See supra* notes 109-13 and accompanying text (providing an overview of short form notice requirements).

207. *See supra* notes 94-107 and accompanying text (providing an overview of full privacy notice requirements).

208. *See, e.g.,* COMPAQ, PROLIANT SERVERS: SELECTING MEMORY (illustrating various storage options for servers), *at* http://www.compaq.com/products/servers/options/memory/selector.html (last visited Feb. 19, 2002); COMPAQ, PROLIANT 6500 MEMORY SELECTOR (detailing the memory of one server in the Compaq line to be 4092 megabytes), *at* http://www.compaq.com/products/servers/options/memory/6500.html (last visited Feb. 19, 2002).

209. For a comparison of average server capacities and security options, see Sun Fire Servers Comparison Chart, *at* http://www.sun.com/servers/comparison/sunfire/index.html (last visited Feb. 19, 2001). Note that the "Sunfire 15k" server holds 576 megabytes of space. *Id.*

210. *Id.*

IV. CONCLUSION—TOWARDS A UNIFORM PRIVACY STANDARD

In the post GLBA world, the consumer who provides non-public personal information for an examination of credit,[211] a determination of loan qualification,[212] or a request for financial advice[213] will find little regulatory assurance of adequate notice regarding the privacy of that information. Although the provision and acknowledgment of a short form privacy notice is required by GLBA,[214] this form of notice may not meet every consumer's reasonable expectation to know which institutions are collecting data, the uses of the data, additional recipients of the data, what data is collected and the means by which it is collected.[215] While consumers have the option of taking extra steps to obtain full privacy notices, it may be cost effective and efficient for financial institutions to merely post full privacy notices before a consumer concludes her transaction.[216] To do so would give consumers adequate notice under the fair information practice principles.[217]

Another issue that consumers feel strongly about is their level of choice.[218] At the forefront of this issue is the debate between advocates of the opt out and opt in models.[219] While the opt in model seems to give consumers greater control over what information may be used by financial institutions, it seems that the

---

211. *See, e.g.*, Privacy of Consumer Financial Information, 12 C.F.R. § 216.3(e)(2)(i) (2001).

212. *See, e.g., id.* § 216.3(e)(2)(ii).

213. *See, e.g., id.* § 216.3(e)(2)(iii).

214. *Id.*

215. The 107th Congress introduced two bills that seek to modify the GLBA to provide heightened notice. *See supra* note 74 and accompanying text.

216. Privacy of Consumer Financial Information, 12 C.F.R. § 216.9(e)(1) (2001). The Agencies' regulations state,

> You may reasonably expect that a consumer will receive actual notice if . . . [f]or the consumer who conducts transactions electronically, post the notice on the electronic site and require the consumer to acknowledge receipt of the notice as a necessary step to obtaining a particular financial product or service . . . .

Id.

217. *See supra* note 81 and accompanying text.

218. *See supra* note 125 and accompanying text.

219. *See supra* note 174 and accompanying text. The 107th Congress introduced a number of bills that propose amending the GLBA to include an opt in model. *See supra* note 75 and accompanying text.

argument for it's inefficiency and high cost outweigh any potential benefits.[220] This issue here may be what level of control consumers have over the sharing of non-public information. This issue, however, may be a moot point if consumers are given a more comprehensive initial notice, as well as the power to correct or modify certain types of information given to institutions.

Unfortunately, consumers who wish to access or correct non-public information will find very little in the way of regulatory support.[221] GLBA does not allow consumers the right to access their information.[222] A number of bills have been introduced, by the 107th Congress that seek to provide consumers with increased access to non-personal information.[223] To establish such a procedure for access using an online medium may be cost effective and efficient. It may merely mean setting up access rights via consumer numbers to a database. With emerging technologies such as cold fusion[224] and asp pages,[225] a consumer's freedom of access could be automated, thereby actualizing the fair information practice principle of access.

Finally, GLBA provides no security guarantee for the protection of consumer information.[226] To require financial institutions to treat the security of consumer information on par with customer information may be cost effective and efficient. It could merely mean storing consumer information within the already mandated secure storage systems that are being used to store customer information. In the context of online transactions, this would entail using the same secure servers and databases that are used for customer information.

The proliferation of differing standards through state legislation,[227] the growing concern regarding what privacy rights consumers can expect,[228] and the congressional debate[229] to amend GLBA underscores the need for a national standard of privacy. A

220. *See supra* notes 122-86 and accompanying text.
221. *See supra* notes 187-94 and accompanying text.
222. *Id.*
223. *See supra* note 76 and accompanying text.
224. *See* Macromedia.com, *supra* note 194.
225. *See* ASPWIRE.COM, *supra* note 194.
226. *See supra* note 195-210 and accompanying text.
227. *See supra* notes 168-69 and accompanying text.
228. *See supra* notes 8-10 and accompanying text.
229. *See supra* notes 70, 74-77 and accompanying text.

number of initiatives have been taken in the private sector to use technology in order to proliferate an industry standard that automates user control over personal information. One such initiative is the P3P (the platform for privacy preferences project), developed by the World Wide Web Consortium. According to the Consortium,

> P3P is a standardized set of multiple-choice questions, covering all the major aspects of a Web site's privacy policies. Taken together, they present a clear snapshot of how a site handles personal information about its users. P3P-enabled Web sites make this information available in a standard, machine-readable format. P3P enabled browsers can "read" this snapshot automatically and compare it to the consumer's own set of privacy preferences. P3P enhances user control by putting privacy policies where users can find them, in a form users can understand, and, most importantly, enables users to act on what they see.[230]

While new technologies are promising, the issue is what protections will be afforded to consumers who seek financial transactions via the World Wide Web and at what cost to financial providers. The first step towards balancing public concern with commercial demand is establishing policy goals. The fair information practice principles are worthy goals through which to begin the long and challenging journey towards a national online privacy standard. While there is disagreement as to what specific insurances legislatures should give consumers, it is clear from the legislation[231] being introduced, public opinion,[232] and national debate[233] that citizens are challenging government to insure that financial institutions provide them with adequate notice, reasonable choice, sufficient access, and practical security systems.

---

230. THE WORLD WIDE WEB CONSORTIUM, THE PLATFORM FOR PRIVACY PREFERENCES (P3P) PROJECT, *at* http://www.w3.org/P3P/#what (last visited Feb. 19, 2002).

231. *See supra* notes 74-77, 168, 169 and accompanying text.

232. *See supra* notes 8-10 and accompanying text.

233. *See supra* notes 70-71 and accompanying text.

Perhaps the fair information practice principles of notice, choice, access and security could serve as ideals towards which government should strive.

DAVID ANNECHARICO